

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-34 (Cancelled)

35. (Currently Amended) A system for distributing and maintaining end-user personal profile data in a data communications system, said system providing communication between applications using said personal profile data, the system comprising:

a central protection server storing personal protection profile information, wherein said personal protection profile information stores information for a particular user as to which personal profile data associated with said particular user is accessible by which particular application;

a requesting application ~~for requesting~~ providing an access request to certain personal profile data associated with a particular user, said user being identified by a first user identity;

an information providing application storing said certain personal profile data associated with said user wherein said certain personal profile data are stored separately from said central protection server storing said personal protection profile information;

wherein said central protection server receives said access request for said certain personal profile data from said requesting application and grants or rejects said request by evaluating the associated personal protection profile information for said particular user; and

wherein said requesting application requests said certain personal profile data from said information providing application in response to said central protection server granting said access request.

36. (Previously Presented) The system according to claim 35, wherein there is one access means for each of said requesting application and said information providing application.

37. (Previously Presented) The system according to claim 35, wherein said central protection server provides a second user identity to the requesting application in response to said access request being granted, wherein said second user identity identifies the user within said information providing application and wherein said requesting application requests said certain personal profile data from said information providing application using said second user identity.

38-39. (Cancelled)

40. (Previously Presented) The system according to claim 35, wherein the personal protection profile information is assigned one of a number of security levels, a lowest security level indicating that all personal profile data access is prevented for every application, and a highest security level indicating that all personal profile data is freely available.

41. (Previously Presented) The system according to claim 36, wherein an interface between said requesting application and said respective access means comprises an Application Programmable Interface based on a generic markup language.

42. (Previously Presented) The system according to claim 41, wherein the generic markup language is XML.

43. (Cancelled)

44. (Previously Presented) The system according to claim 35, wherein access to said requested personal profile data is granted or rejected by the central protection server in communication with the information providing application.

45. (Previously Presented) The system according to claim 35, wherein access to said requested personal profile data is granted or rejected by the central protection server in communication with the requesting application and the information providing application.

46. (Cancelled)

47. (Previously Presented) The system according to claim 36, wherein user identity translating means are provided in the access means of the requesting application.

48. (Previously Presented) The system according to any one of claim 35, wherein a general Document Type Definition (DTD) is defined to allow flow of personal data between said requesting application and said information providing application.

49. (Previously Presented) The system according to claim 48, wherein for each user a specific user DTD agreement is given.

50. (Previously Presented) The system according to claim 36, wherein said access request for said personal profile data is transported from the requesting application to its access means using Remote Method Invocation (RMI).

51. (Previously Presented) The system according to claim 50, wherein the request is transported as an XML transport object tagged with information about the requested end-user personal profile data.

52. (Previously Presented) The system according to claim 50, wherein an HTTPS protocol is used for communication between the access means of the requesting or information holding application and the central protection server.

53. (Previously Presented) The system according to claim 36, wherein the access means of the information requesting or providing application includes means for encrypting the first user identity.

54. (Previously Presented) The system according to claim 36, wherein the request is digitally signed with at least one of a private key of the access means of the requesting application and a private key of the access means of the information providing application.

55. (Previously Presented) The system according to claim 54, wherein the request is digitally signed with a private key of the central protection server, and in that the digital signature of the access means are verified in the central protection server.

56. (Previously Presented) The system according to claim 55, wherein the central server means comprises means for encrypting at least the second user identity used by the information providing application.

57. (Previously Presented) The system according to claim 35, wherein at least some of the applications include respective cache memory respectively for temporarily holding information about access requests, and a previously used session can be reused at least for a given time period.

58-62. (Cancelled)

63. (Previously Presented) A method of controlling access to personal profile

data in a data communication network running a number of applications having or communicating with information holding means, the method comprising the steps of:

providing an access request for a particular personal profile data for a particular user from a requesting application to an access means associated with said requesting application using a generic mark-up language,

forwarding the access request from the access means to a central server means storing personal protection profile information for said particular user, wherein said personal protection profile information stores information for said user as to which portion of said personal profile data are accessible to which particular application within said network;

establishing whether access to said requested personal profile data is to be granted or denied by using the request and the personal protections profile information at said central server means,

if access to the requested personal profile data is to be granted, confirming to the access means of the requesting application that access is to be granted after digitally signing the request; and

allowing transfer of an encrypted and digitally signed request to an information providing application storing said requested personal profile data, wherein said personal profile data are stored separately from said central server means storing said personal protection profile information.

64. (Previously Presented) The method according to claim 63, further comprising the steps of:

receiving a first user identity from said requesting application at said central server means;

translating said first user identity to a second user identity recognizable by said information providing application; and

providing said second user identity, while not disclosing said first user identity, to said information providing application.

65. (Previously Presented) The method according to claim 63, wherein the access request of said requesting application relates to setting or updating data in said personal profile data, for a granted request, the method further comprises the step of:

transferring the data to be set or updated to the information providing application over the data communication network.

66. (Currently Amended) A method of controlling access to personal profile data in a data communication network running a number of applications having or communicating with information holding means, the method comprising the steps of:

forwarding a request for access to personal profile data for a particular user from a requesting application to a central server means;

establishing in the central server means for determining whether access to said requested personal profile data should be allowed or not by comparing the request with an end-user controlled personal protection profile, wherein said personal protection profile indicates which portion of personal profile data associated with said user can be accessed by which application within said network; and

providing information as to whether said request is allowable or not, such that if said request is allowable, the data communication network can be used for giving the requesting application access to the requested personal profile data without the identity of the requesting application being visible to an information providing application providing the requested personal profile data, wherein an identity of said information providing application is further concealed from said requesting application.

67. (Previously Presented) The method according to claim 66, further comprising the steps of:

receiving a first user identity transmitted by said requesting application at said central server means;

translating said first user identity associated with said user to a second user identity recognizable by said information providing application; and

communicating with said information providing application using said second user identity in order to prevent the disclosure of said first user identity to said information providing application.

68. (Previously Presented) The method according to claim 66, further comprising the steps of:
digitally signing the request transmitted by the requesting application.

* * *